

# EUROPEAN BANKING GUIDE FOR NONPROFITS

## *HOW TO OPEN AND MANAGE AN ORGANIZATIONAL BANK ACCOUNT*



European Center for  
Not-for-Profit Law



**PILnet**



**DENMARK**

*Partnering firms participating in this research are not liable towards third parties for the accuracy of the information contained in this guide. The research cannot be considered as legal advice. It was carried out in 2022 and responds to the regulatory framework on organizational banking in this time period. If you have further queries please reach out to our clearinghouse for legal help.*



European Center for  
Not-for-Profit Law

### **European Center for Not-for-Profit Law Stichting (ECNL)**

ECNL's mission is to create legal and policy environments that enable individuals, movements and organizations to exercise and protect their civic freedoms and to put into action transformational ideas that address national and global challenges. We envision a space in which everyone can exercise their rights freely, work in solidarity and shape their societies.



### **PILnet**

PILnet is a global non-governmental organization that creates opportunities for social change by unlocking law's full potential. With programs in Europe & Eurasia, Asia, and at the global level, PILnet aims to reclaim and reimagine the role of law so that it works for the benefit of all. PILnet builds networks and collaborations of public interest and private lawyers who understand how law works when it serves the interests of the privileged and then it uses that knowledge to strengthen civil society and the communities they serve. PILnet not only obtains high-quality, free legal assistance for civil society organizations when they urgently need it but also helps organizations to capitalize on the full range of specialized legal expertise that can be provided by corporate lawyers, including against ongoing, or even yet-to-be-determined, challenges.

© 2022 by the European Center for Not-for-Profit Law Stichting (ECNL), PILnet and Partnering Firms.

# 1. OPENING AN ORGANIZATIONAL BANK ACCOUNT

## a. What are the requirements to open an organizational bank account?

### i. Do organizations have to be physically present in the country to open a bank account? I.e., can they operate in country X but have a bank account in country Y?

No. It is not a requirement under Danish law that organizations have to be physically present in Denmark to open a bank account. A CSO that operate in a country other than Denmark may therefore apply for and open a bank account with a bank in Denmark.

### ii. Are there specific requirements for CSOs to open accounts by law or asked in practice by the banks (e.g, years of operations, annual turnover, to have director or member of governing body to be national of the country)

Danish law does not contain any specific procedural requirements or formalities with respect to opening a bank account in Denmark.

However, when opening a bank account for a CSO, the relevant bank will establish a “business relationship” with the CSO and must therefore comply with the requirements on customer identification and due diligence in the Danish Act on Measures to Prevent Money Laundering and Financing of Terrorism (the “AML Act”) with respect to the relevant CSO.

We refer to our response to section 2 below for further information on the relevant requirements pursuant to the AML Act.

### iii. Who is authorized/required to open a bank account? Can this be done online, or that person needs to be present in the country? In case of requirement of presence can this be fulfilled by signing the paperwork at an embassy or notary?

Banks would normally require account opening agreements be signed by authorised signatories on behalf of the CSO. The documents can usually be signed electronically and there are no

legal requirements under Danish law for the documents to be signed in presence of a witness or notary or similar formalities. However, some banks may require a meeting (physical or online) to be held with representatives of the CSO before opening a bank account, especially if the CSO in question does not have a permanent establishment or representative in Denmark.

**iv. What is the process of setting up a bank account? E.g., how long it takes, is there a practice to have an interview in the bank?**

Generally, we would expect the process of setting up a bank account to take anything between 2 weeks and up to 3 months, depending on the time it takes for the bank to complete satisfactory customer identification and due diligence procedures.

## **2. BANKING ACTIVITIES**

**a. What customer due diligence requirements are in place and what is their impact on civil society organizations' banking activities?**

Section 11 of the AML Act stipulates the general requirements for customer due diligence procedures, which, inter alia, entails that the relevant bank must:

1. obtain identity details on the CSO;
2. verify the identity details obtained via an independent and reliable source;
3. identify the ownership and control structure of the CSO and obtain identity details on the CSO's beneficial owner(s) and implement reasonable measures to verify the identity of the beneficial owner(s).

**1. Obtaining identity details**

If the CSO is a legal person, its name and central business registration (CVR) number must be obtained. If the CSO in question does not have a CVR number, similar identity details must be obtained. For foreign undertakings, other forms of identification details can be a registration number, e.g. TIN number (Tax Identification Number), LEI code (Legal Entity Identifier) or another unique registration number. If the CSO has

no CVR number or similar, it is a requirement that the bank at least has details of the CSO's legal status (form of incorporation), e.g. if a limited liability company, a foundation, trust or other.

## **2. *Verifying identity details***

The identity details the bank has obtained on the CSO must be verified on the basis of documents, data or details obtained from a reliable and independent source. This means that verification of the CSO's identity must be done through a source other than the CSO. The reliable source can be a public authority, but it can also be another reliable external source. It is also important that the source is current. The extent of documentation, data or information providing adequate verification of a CSO's identity details is a specific evaluation. But there can be no reason to doubt that the CSO is the legal person that it claims to be. In this connection, the bank must risk assess its customers, which can mean that enhanced customer due diligence procedures must be conducted.

Verification for legal persons can consist of e.g. a search in the CVR (Central Business Register), details from the Danish Tax Agency, or a copy of the certificate of incorporation and articles of association. If the CSO is established outside Denmark, similar details from corresponding public authorities or registers can be used to verify the CSO's identity details. For CSOs without a registration number, e.g. certain associations, verification can be performed by obtaining a copy of the deed of foundation and articles of association if available, supplemented by details on the persons who can act on behalf of the association. A deed of foundation can, for example, be a copy of the minutes from the founding general meeting.

## **3. *Ownership and control structure and beneficial owners***

When the bank's customer is a legal person (including an association), the bank must identify its ownership and control structure. Clarification of a customer's ownership and control structure will help determine who are the customer's beneficial owners.

A customer's beneficial owner is the natural person(s) who ultimately own or control the customer, or the natural person(s) on whose behalf a transaction or activity is conducted. Beneficial owners can be natural persons, and the bank must identify the full ownership and structure chain, and determine who ultimately owns or controls the customer.

The principle is that the customer has beneficial owners, and can identify them. There are however instances when there are no natural persons who own and/or control the customer to a sufficient degree to be defined as beneficial owners. In such instances, the customer's general management will be regarded as the beneficial owner(s) instead. This can be, for example, when a customer is an association that does not have beneficial owners. In such cases, it is as a main rule the general management that must be considered the beneficial owners of the association.

In associations, such as CSOs, it will therefore often be the board of directors or executive board (if they have one) that will comprise the association's general management, and that will therefore be regarded as the beneficial owners. But it will depend on specific risk assessment of each association/CSO and its status. To help identify the beneficial owners, the bank can obtain the deed of foundation, articles of association or minutes from the general meeting.

The bank's customer due diligence procedures can be conducted based on a risk assessment of the specific customer relationship.

**b. Which internal principles or official (central bank) "suspicious transaction" monitoring criteria are in place affecting the civil society organizations? Is it publicly available?**

Besides the requirements pursuant to the AML Act (described below), there are no official/public "suspicious transaction" monitoring criteria in place affecting CSOs.

Pursuant to Section 25(1) of the AML Act, all banks have a duty to investigate the background and purpose of transactions, transaction patterns and activities when there may be a suspicion or reasonable cause to believe that they are, or have been, linked to money laundering or terrorist financing.

The purpose of investigation is to determine whether there is a suspicion or reasonable cause to suspect that a transaction or activity is, or has been, linked to money laundering or terrorist financing. This means that banks must have business procedures and systems in place that make it possible to identify such transactions and activities. Banks must thus investigate the background and purpose of all transactions, transaction patterns and unusual activities that are complex, unusually large, carried out in an unusual pattern or do not have an obvious economic or legal purpose.

If the bank believes that an enquiry to the customer about a transaction will inform the customer that the bank is suspicious and is in the process of conducting an investigation, or if the bank deems it inappropriate to contact the customer on the matter, the bank must report to the the Danish Money Laundering Secretariat (*Hvidvasksekretariatet*) (“MLS”). If the bank cannot completely disprove its suspicion, notification must also be made. The bank must be aware that the requirement implies that suspicion must be disproved if no notification is required. It is therefore not enough that suspicion has only been reduced.

A report must be made to the MLS if the bank knows or suspects or has reasonable reason to suspect that a transaction or activity is or has been associated with money laundering or terrorist financing. The MLS must be notified immediately. The bank must thus deal with suspicious transactions and activities in a manner that accelerates the process as much as possible. “The process” is defined as the stage from monitoring customer transactions and detecting something suspicious, to investigation and determining that the suspicion can be regarded as confirmed. The duty to report also applies in connection with attempts to carry out a transaction or a request from a potential customer that wants to perform a transaction or activity, e.g. opening of a bank account. Refused requests must therefore also be reported if the bank considers that there is an attempt at money laundering or terrorist financing involved.

The bank has a duty of confidentiality concerning a report given or considered. This means that a data subject has no right of access to reports made to the MLS concerning themselves.

### **c. Do the banks in the country of operations have any restrictions/limitations to bank transactions and transfers to certain jurisdictions (such as high-risk ones).**

Yes, banks usually have internal restrictions/limitations for transactions and transfers to certain jurisdictions for purposes of ensuring compliance by the bank with both its ongoing monitoring obligations under the AML act as well as any restrictive measures imposed by the EU against certain countries, regimes, persons and entities.

If a bank finds a match when screening a customer or transaction, for example, when the name of the customer or the transaction recipient matches an individual, group, legal entity or body that is subject to freezing, the bank must investigate

whether this is just a name match or also an identity match. An identity match means that the customer or the transaction recipient is listed in one of the regulations, and therefore no funds must be made available to that individual, group, legal entity or body. In the case of an identity match, the bank must therefore not open accounts, invest, transfer or otherwise give the individual access to the financial market.

We would generally expect Danish banks to have in place internal restrictions/limitations that would prevent transactions and transfers to jurisdictions that are listed on FATF's black list as well as systems that monitors transactions and transfers to jurisdictions that are listed on FATF's grey list.

### 3. OBLIGATIONS AND REPORTING REQUIREMENTS

#### **a. Are banks required to provide CSO clients' financial information to CSO regulatory authorities or public officials? If yes, under what circumstances must banks do so, and what types of information must they provide?**

Section 117(1) of the Danish Financial Business Act prohibits unjustified disclosure of confidential information by financial undertakings. As a general rule, all customer information is confidential. The starting point is therefore that banks are not permitted to disclose customers' financial information to regulatory authorities, public officials or other third party recipients, unless the disclosure is "justified".

It depends on an individual assessment, based on the bank's interest in disclosing the information and the customer's justified expectation that the information is kept confidential, whether disclosure to another recipient is justified. Disclosure of customer information to another recipient may, for example, be justified if the bank according to law is obliged to disclose the information or if the customer specifically consents to the disclosure of the relevant information. For example, a bank is obliged to disclose information about its customers that are



necessary for the Danish Financial Supervisory Authority to carry out its activities, including, but not limited to, monitoring compliance with the AML Act. Further, a bank is obliged to disclose certain information about its customers to the Danish Tax Authorities.

**b. What obligations do banks have to protect the privacy of clients' information?**

Banks are obliged to comply with the General Data Protection Regulation (“GDPR”) when processing personal data about its customers. Banks will therefore also have in place data processing policies setting out which types of data the bank process and store and for which purposes, the legal basis for such processing of personal data, the customer’s rights, information about the data controller etc.

All personal data, including, for example, information on the customer’s beneficial owners, which the bank obtains according to the AML Act, can only be processed by the bank in accordance with the AML Act and not for any other purposes.

**c. Are there specific reporting obligations for banks to inform governments on civil society banking in certain circumstances?**

We refer to our response to section 2(b) above where it is outlined under which circumstances a bank is obliged to notify the MLS.

**d. Are you aware of any change in regulation/practice due to the Russian sanctions?**

It is a general impression that enforcement of sanctions relating to Russia appears highly prioritized by banks and that the banks have adopted a very cautious approach to enforcement with the aim to eschew risk as they navigate the sanctions. In that regard, the sanctions seem to have had a “chilling effect” on customers and transactions with a proximity to Russia or Russian individuals/entities, as the threat of legal sanction, even if only remote, simply discourage banks from carrying out otherwise legitimate transactions.



European Center for  
Not-for-Profit Law

European Center for Not-for-Profit Law Stichting  
5 Riviervismarkt, 2513 AM  
The Hague, Netherlands  
[www.ecnl.org](http://www.ecnl.org)  
[twitter.com/enablingNGOlaw](https://twitter.com/enablingNGOlaw)



PILnet  
199 Water Street, 11th Floor  
New York, NY 10038 U.S.A.  
<https://www.pilnet.org>  
[twitter.com/PILnet](https://twitter.com/PILnet)